ISO 27001:2022 改版簡介

杜貴忠

ISO 27001:2022

如何改變

主條文差異

附錄A的改變

如何遵循新標準

結論

主條文差異

ISO 27001:2022

主條文差異

ISO 27001:2022

1.名稱

2.頁數

3.術語與定義(參考資訊)

4.新增要求(4.2瞭解利害關係方的需求與期望)

5.強化過程導向(4.4資訊安全管理系統)

6.新增要求(6.2資訊安全目標與達成之規劃)

7.新增要求(6.3變更規劃)

8.簡化要求(7.4溝通)

9.新增要求(8.1運作的規劃與控管)

10.新增要求(9.1 監督、量測、分析與評估)

11.要求架構變更(9.2、9.3)

12.要求架構變更(10.改善)

1.名稱

ISO 27001:2013

ISO/IEC 27001:2013

Information technology — Security techniques — Information security management systems — Requirements

資訊技術 - 安全技術 - 資訊安全管理系統 - 要求事項

ISO 27001:2022

ISO/IEC 27001:2022

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

資訊安全 - 網路安全與隱私保護 - 資訊安全管理系統 - 要求事項

2.頁數

ISO/IEC 27001:2013

23

ISO/IEC 27001:2022

19

3.術語與定義(參考資訊)

ISO/IEC 27001:2013

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

ISO/IEC 27001:2022

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp
— IEC Electropedia: available at https://www.electropedia.org

4.新增要求(4.2瞭解利害關係方的需求與期望)

ISO 27001:2013

4.2 了解利害關係者的需求與期望

組織應決定：

a)與ISMS有關的利害關係者；以及

b)這些利害關係者對資訊安全之要求。

備考：這些利害關係者的要求可能包含了法規要求與契約義務。

ISO 27001:2022

4.2 瞭解利害關係方的需求與期望

組織應確定：

a)與資訊安全管理系統相關的利害關係各方;

b)這些利害關係方的相關要求;

C)將如何經由資訊安全管理系統滿足前述相關要求。

備考：利害關係方的要求可能包括法律和法規要求以及合約義務。

5.強化過程導向(4.4資訊安全管理系統)

ISO 27001:2013

4.4 資訊安全管理系統

組織應依據本標準的要求，以建立、實施、維護和持續改進ISMS。

ISO 27001:2022

4.4 資訊安全管理系統

組織應根據本標準的要求建立、實施、維護和持續改進資訊安全管理系統，包括所需的過程及其互動。

6.新增要求(6.2資訊安全目標與達成之規劃)

ISO 27001:2013

6.2 資訊安全目標與達成之規劃

組織應在相關的功能與層級中建立資訊安全目標。

資訊安全目標應：

a)與資訊安全政策一致；

b)可測量（如果可行時）；

c)考量適用的資訊安全要求，以及風險評鑑與處理結果；

d)經過溝通，且

e)適當時作更新。

ISO 27001:2022

6.2 資訊安全目標與達成之規劃

組織應在相關的功能與層級中建立資訊安全目標。

資訊安全目標應：

a)與資訊安全政策保持一致;

b)可以量測（如果可行）;

c)考慮適用的資訊安全要求，以及風險評估和風險處理的結果;

d)受到監控;

e)被傳達;

f)適時更新;

g)作為記錄的文件化資訊提供。

7.新增要求(6.3變更規劃)

6.3 變更規劃

當組織確定需要對資訊安全管理系統進行變更時，應以預先規劃的方式進行變更。

ISO 27001:2013 無此項要求

8.簡化要求(7.4溝通)

7.4 溝通

組織應決定與ISMS有關的內部與外部溝通之需求，包含：

a)溝通什麼；

b)何時溝通；

c)和誰溝通；

d)誰應溝通；以及

e)應實現哪種溝通過程。

ISO 27001:2013

7.4 溝通

組織應決定與ISMS有關的內部與外部溝通之需求，包含：

a)溝通什麼；

b)何時溝通；

c)和誰溝通；

d)如何溝通。

ISO 27001:2022

9.新增要求(8.1運作的規劃與控管)

ISO 27001:2013

8.1 運作的規劃與控管

組織應規劃、實施與控管可符合資訊安全要求，及實施在條文6.1所決定的行動。組織也應實施計畫，以達成在條文6.2所決定的資訊安全目標。

組織應依照計畫實現過程所必需的信心程度，保存文件化資訊。

組織應管制計畫的變更，並審查無預期的變更會帶來的後果，在必要時，採取措施以減輕任何不良影響。

組織應確認委外之過程是被建立及控管。

ISO 27001:2022

8.1 運作之規劃及控制

組織應策劃、實施和控制滿足要求所需的過程，並通過以下方式實施第 6 章確定的措施：

—為過程建立準則；

—根據準則實施過程控制。

組織應保存文件化資訊，其程度必須具有足以達成其過程已依規劃執行之信心。

組織應控制所規劃之變更，並審查非預期變更之後 果，必要時採取行動以減輕任何負面效果。

組織應確保與有關於資訊安全管理系統由外部提供的過程、產品或服務受到控制。

10.新增要求(9.1 監督、量測、分析與評估)

ISO 27001:2013	ISO 27001:2022
9.1 監督、量測、分析與評估 組織應評估資訊安全的績效與ISMS的有效性，並決定：..... 組織應保存適當的文件化資訊，以作為監督與量測結果的證據。	9.1 監督、量測、分析與評估 組織應評估資訊安全的績效與ISMS的有效性，並決定：..... 組織應保存適當的文件化資訊，以作為監督與量測結果的證據。 **組織應評估資訊安全績效及資訊安全管理系統之有效性。**

11.要求架構變更(9.2、9.3)

ISO 27001:2013

9.2 內部稽核

9.3 管理階層審查

ISO 27001:2022

9.2 內部稽核

- 9.2.1 一般要求
- 9.2.2 內部稽核方案

9.3 管理審查

- 9.3.1 一般要求
- 9.3.2 管理審查輸入事項
- 9.3.3 管理審查結果

新增輸入事項：c)與資訊安全管理系統有關的利害關係方的需求和期望的變化；

12.要求架構變更(10.改善)

ISO 27001:2013

10.1 不符合事項與矯正措施

10.2 持續改善

ISO 27001:2022

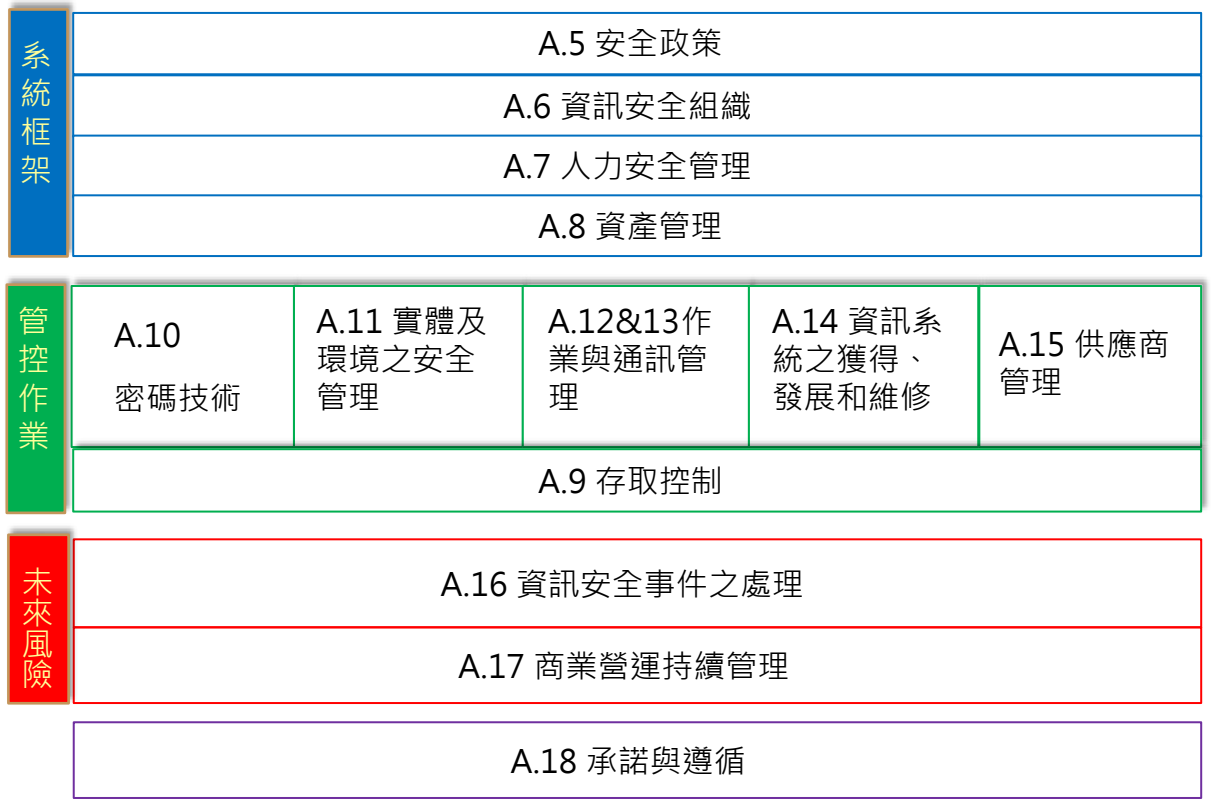
10.1 持續改善

10.2 不符合事項與矯正措施

附錄A的改變

ISO 27002:2022

1.整體架構



ISO 27002:2013

ISO 27002:2022

2.控制措施屬性

01 控制措施種類

用於從控制措施**何時以及如何修改**與資訊安全事故發生的**相關風險**之觀點來檢視控制措施。屬性值包括**預防性**、**偵測性**和**矯正性**。

02 資訊安全特性

用於從控制措施將**有助於保留資訊的哪些特徵**之觀點來檢視控制措施。屬性值包括**機密性**、**完整性**和**可用性**。

03 網路安全概念

網路安全概念是從與 ISO/IEC TS 27110 中描述之網路安全框架中定義的**網路安全概念之控制措施**所關聯的觀點來檢視控制措施的屬性。屬性值包括**識別**、**保護**、**偵測**、**回應**和**復原**。

04 運作能力

運作能力是從**資訊安全能力的實踐者觀點**來檢視控制措施的一個屬性。屬性值包括**治理**、**資產管理**、**資訊保護**、**人力資源安全**、**實體安全**、**系統與網路安全**、**應用程式安全**、**安全組態**、**身份與存取管理**、**威脅與弱點管理**、**持續性**、**供應商關係的安全**、**適法與遵循性**、**資訊安全事件管理**和**資訊安全保障**。

05 安全領域

安全領域是從四個**資訊安全領域**的觀點來檢視控制措施的屬性，屬性值包括**治理與生態系統**、**保護**、**防禦**與**復原力**。

2.控制措施屬性範例

5 組織面控制措施

5.1 資訊安全政策

控制措施種類	資訊安全特性	網路安全概念	運作能力	安全領域
#預防性	#機密性 #完整性 #可用性	#識別	#治理	#治理與生態系統 #復原力

5.2 資訊安全的角色與職責

控制措施種類	資訊安全特性	網路安全概念	運作能力	安全領域
#預防性	#機密性 #完整性 #可用性	#識別	#治理	#治理與生態系統 #保護 #復原力

3.控制措施內容架構

6.1.3 與權責機關之聯繫

控制措施

宜維持與相關權責機關之適切聯繫。

實作指引

組織宜備妥程序，規定宜聯繫權責機關(例：執法單位、監理機關及主管機關)之時機及人員，以及已識別之資訊安全事故，宜如何以及時方式通報(例：若有違法疑慮)。

其他資訊

可能受網際網路攻擊之組織，可能需權責機關採取作為以抵禦攻擊源。

維護此等聯繫可能係支援資訊安全事故管理(參照第 16 節)或營運持續及應變規劃過程(參照第 17 節)之要求事項。與監理機關之聯繫，對組織必須實作之法律或法規即將變更的預測及準備亦有助益。與其他權責機關之聯繫，包括公用事業(utility)、緊急服務、電力公司及醫療衛生與安全，例：消防部門(與營運持續有關)、電信業(與線路選路及可用性有關)、水公司(與設備之冷卻設施有關)等。

ISO 27002:2013

5.5 與權責機關的聯繫

控制措施種類	資訊安全特性	網路安全概念	運作能力	安全領域
#預防性 #矯正性	#機密性 #完整性 #可用性	#識別 #保護 #回應 #復原	#治理	#防禦 #復原力

控制措施

組織應與有關之權責機關建立並保持聯繫。

目的

確保組織與相關法律、監管和監督機構之間在資訊安全方面進行適當的資訊流通。

指引

組織應指定何時和由誰聯繫權責機關（例如執法、監管機構、監督機構），以及如何及時報告已識別的資訊安全事件。

並且，應透過與權責機關的聯繫來促進了解這些權責機關當前和未來的期望（例如適用的資訊安全法規）。

其他資訊

受到攻擊的組織可以請求權責機關對攻擊來源採取行動。

保持此類聯繫可能是支援資訊安全事件管理的必要條件（見 5.24 至 5.28）或應變計劃和營運連續性之過程（見 5.29 和 5.30）。與監管機構的聯繫也有助於預測和準備即將發生之影響組織的相關法律或法規變化。與其他權責機關的聯繫包括公用事業、緊急服務、電力供應商以及健康和安全[例如消防部門（與營運連續性有關）、電信提供商（與線路路由和可用性有關）和供水商（與設備冷卻設施有關）]。

ISO 27002:2022

3.控制措施數量

114項控制措施

95項控制措施

3.控制措施數量(新增11項)

5.7	威脅情資
5.23	使用雲端服務之資訊安全
5.30	為營運持續性做好資通技術(ICT)的準備
7.4	實體安全監控
8.9	組態管理
8.10	資訊刪除
8.11	資料遮蔽
8.12	預防資料洩漏
8.16	活動監控
8.22	網頁過濾
8.28	安全編碼

4.新增(5.7 威脅情資)

控制措施

應蒐集和分析與資訊安全威脅有關的資訊以產出威脅情資

目的

提供對組織之威脅環境的認知，以便組織得以採取適當的緩解行動。

指引

蒐集並分析有關現存或新興威脅的資訊，以使：
a)促進具見識的知情行動，以防止威脅對組織造成傷害；
b)減少此類威脅的衝擊。

實務做法

1. 訂定威脅情資作業程序
2. 選擇來源，例如：TWCERT、CVE等
3. 管控協威脅情資之蒐集、分析、處理、運用、溝通及分享。
4. 建議修訂資安事件程序書

4.新增(5.23使用雲端服務之資訊安全)

控制措施

應根據組織的資訊安全要求建立獲取、使用、管理和退出雲端服務的流程。

目的

為雲端服務的使用明訂和管理資訊安全。

指引

組織應建立並就使用雲端服務的特定主題政策與所有利害關係者進行溝通。

組織應定義並傳達其打算如何管理與雲端服務之使用所相關的資訊安全風險。

實務做法

1. 訂定雲端服務作業程序(委外作業程序)
2. 選擇服務、訂定協議、管控安全、定期查核、服務水準、日誌紀錄、變更管理、安全退出。
3. 風險分析、營運持續。
4. 建議修訂委外作業程序書

4.新增(5.30為營運持續性做好資通技術(ICT)的準備)

控制措施	目的	指引	實務做法
應基於營運持續性目標和 ICT 持續性要求來規劃、實施、維護並測試 ICT 準備情形。	確保當發生中斷時，組織資訊和其它相關資產的可用性。	組織應確保以下： a) 有適當的組織架構，以準備、減輕和因應由具有必要責任、權力與能力的人員來支援發生的中斷； b) ICT持續性計劃，包括詳細說明組織計劃如何管理ICT服務中斷的因應和恢復程序 c) ICT持續性計劃。	1. 訂定ICT持續性計劃(以業務流程分析資訊系統)。 2. 設定營運持續編組。 3. 執行演練驗證計劃是否可行。 4. 建議修訂營運持續管理程序書

4.新增(7.4實體安全監控)

控制措施	目的	指引	實務做法
應持續監控場域以避免未經授權的實體存取。	偵測和阻止未經授權的實體存取。	應持續監控對容納關鍵系統之建築物： a) 安裝影像監控系統，例如閉路電視，以查看並記錄對組織場域內外敏感區域的存取 b) 根據相關適用標準安裝並定期測試接觸、聲音或移動偵測器以觸發入侵者警報 c) 使用這些警報覆蓋所有對外出入口和可存取的窗戶。無人區應隨時保持可告警狀態。	1. 安裝門禁、監控及警報系統。 2. 執行進出管制、定期查核、告警事件處理、記錄保存。 3. 系統應定期測試監控安全 4. 建議修訂實體環境程序書。

4.新增(8.9組態管理)

應建立、文件化、實施、監控和審查硬體、軟體、服務和網路的組態，包括安全組態

控制措施

確保硬體、軟體、服務和網路在所需的安全設定下正常運行，並且組態不會因未經授權或不正確的變更而遭到異動。

目的

組織應定義和實施流程和工具，以為硬體、軟體、服務（例如雲端服務）和網路、新安裝的系統以及運作中的系統於其生命週期內執行定義好的組態（包括安全組態）。

指引

1. 進行資產盤點時應清點其組態分類。
2. 建立各項組態基準，並依基準執行組態管理
3. 確認各項基準現狀及變更。
4. 建議修訂資訊資產管理程序書，或新增組態管理程序書

實務做法

4.新增(8.10資料刪除)

當不再需要時，應刪除儲存於資訊系統、裝置或任何其它儲存媒體中的資訊。

控制措施

防止不必要的敏感資訊揭露，並遵守有關資訊刪除的法令法規、監管與合約要求。

目的

當刪除系統、應用程式與服務上的資訊時，應考慮以下幾點：
a)根據營運需求並考慮相關法令法規，以選擇刪除方法（如電子覆寫或加密抹除）；
b)記錄刪除結果以作為證據；
c)當採用服務供應商的資訊刪除服務時，向其獲取資訊刪除的證據。

指引

1. 進行資產盤點時應清點資訊保存週期。
2. 建立各類型資料刪除方式、週期及記錄格式。
3. 執行刪除並保存紀錄。
4. 建議修訂資訊資產管理程序書，或新增資訊管理程序書

實務做法

4.新增(8.11資料遮蔽)

應根據組織關於存取控制與其它相關的特定主題政策以及營運要求使用資料遮蔽，並將法律要求納入考量。

控制措施

限制敏感資料（包括PII）的揭露，並遵守法令法規、監管和合約要求。

目的

當需要考慮保護敏感資料（例如PII）時，組織應考量使用資料遮蔽、擬匿名化或匿名化等技術隱藏此類資料。
擬匿名化或匿名化技術可以隱藏PII，掩飾PII當事人或其它敏感資訊的真實身份、斷開PII與PII當事人身份或其他敏感資訊之間的連結。

指引

1. 進行資產盤點時應確認資訊是否進行遮蔽。
2. 建立各類型資料遮蔽方式及記錄格式。
3. 執行遮蔽並保存紀錄。
4. 建議修訂資訊資產管理程序書，或新增資訊管理程序書

實務做法

4.新增(8.12預防資料洩漏)

資料洩漏的預防措施應應用於處理、儲存或傳輸敏感資訊的系統、網路及任何其它裝置。

控制措施

檢測並防止個人或系統未經授權地揭露和提取資訊。

目的

組織應考慮以下事項以降低資料洩露的風險：
a) 識別和分類資訊以防止洩露（例如個人資訊、訂價模式和產品設計）；
b) 監控資料洩漏管道（例如電子郵件、檔案傳輸、行動設備和可攜式儲存裝置）；
c) 採取措施防止資訊洩露（例如，隔離包含敏感資訊的電子郵件）。

指引

1. 進行資產盤點時應識別及分類。
2. 整合各項資訊洩漏防護措施。
3. 利用控制措施屬性，管控資訊保護做法。
4. 建議修訂資訊資產管理程序書，或新增資訊管理程序書

實務做法

4.新增(8.16活動監控)

控制措施	目的	指引	實務做法
應監測網路、系統和應用程式的異常行為，並採取適當行動以評估潛在的資訊安全事故。	偵測異常行為和潛在的資訊安全事故。	監控範圍和級別應根據業務和資訊安全要求並結合相關法律法規確定。 應使用通過監測工具進行的持續監測。應根據組織的需要和能力，即時或定期進行監控。 應將異常事件傳達給相關方，以改進以下活動：稽核、安全評估、漏洞掃描和監控（見 5.25）。 應制定程式以及時回應來自監控系統的積極指標，以儘量減少資安事件（見 5.26）對資訊安全的影響。	1. 檢討現有監控工具，若有不足宜購置相關工具。 2. 整合監控、漏洞及資安事件通報。 3. 針對監控紀錄執行分析、處理及運用。 4. 修訂資安事件程序書、作業安全程序書。

4.新增(8.22網頁過濾)

控制措施	目的	指引	實務做法
應管理對外部網站的存取，以減少曝露於惡意的內容。。	保護系統免受惡意軟體的危害並防止存取未經授權的網頁資源。	組織應降低員工存取包含非法資訊或已知包含病毒或網路釣魚材料的網站的風險。一種通過阻止相關網站的 IP 位址或域來實現此目的的技術。一些流覽器和反惡意軟體技術會自動執行此操作或可以配置為執行此操作。 組織應確定人員應該或不應該訪問的網站類型。 在部署此控制之前，組織應建立安全和適當使用線上資源的規則，包括對不受歡迎或不適當的網站和基於網站的應用程式的任何限制。	1. 檢討現有防火牆或網路控制工具，依照指引執行相關設定。 2. 教育訓練教材中應放入本項控制措施。 3. 定期檢討各項限制規則，並更新規則。 4. 修訂網路安全程序書。

4.新增(8.28安全編碼)

控制措施	目的	指引	實務做法
軟體開發應採用安全編碼原則。	確保安全編寫軟體，從而減少軟體中潛在資訊安全漏洞的數量。	組織應建立組織範圍的流程，為安全編碼提供良好的管理。應建立和應用最低安全基準。此外，此類流程和管理應擴展到涵蓋來自協力廠商的軟體元件和開源軟體。 組織應監控現實世界的威脅以及有關軟體漏洞的最新建議和資訊，以通過持續改進和學習來指導組織的安全編碼原則。這有助於確保實施有效的安全編碼實作，以應對快速變化的威脅形勢。	1. 檢討現有軟體開發流程，將安全要求導入開發過程中。 2. 管控各項元件(含第三方)之安全性。 3. 執行必要的測試及安全性檢測工作。 4. 結合構型管理。 5. 修訂資訊系統開發維護程序書。

3.控制措施數量(整合合併24項)

2022	2013	項目名稱
5.1	05.1.1、05.1.2	資訊安全政策
5.8	06.1.5、14.1.1	專案管理中的資訊安全
5.9	08.1.1、08.1.2	資訊和其它相關資產的清查盤點
5.10	08.1.3、08.2.3	資訊和其他相關資產的可接受使用
5.14	13.2.1、13.2.2、	資訊傳遞
5.15	09.1.1、09.1.2	存取控制
5.17	09.2.4、09.3.1、	認證資訊
5.18	09.2.2、09.2.5、	存取權限
5.22	15.2.1、15.2.2	供應商服務之監控、審查及變更管理
5.29	17.1.1、17.1.2、17.1.3	中斷期間的資訊安全
5.31	18.1.1、18.1.5	識別法令法規、監管與合約要求
5.36	18.2.2、18.2.3	資訊安全政策、規則與標準之遵循性
6.8	16.1.2、16.1.3	資訊安全事件通報
7.2	11.1.2、11.1.6	實體進出管制
7.10	08.3.1、08.3.2	儲存媒體
8.1	06.2.1、11.2.8	使用者端點設備
8.8	12.6.1、18.2.3	技術漏洞的管理
8.15	12.4.1、12.4.2	日誌存錄
8.19	12.5.1、12.6.2	在作業系統上安裝軟體
8.24	10.1.1、10.1.2	密碼學的使用
8.26	14.1.2、14.1.3	應用程式安全要求
8.29	14.2.8、14.2.9	開發與驗收的安全測試
8.31	12.1.4、14.2.6	區隔開發、測試與正式環境
8.32	12.1.2、14.2.2	變更管理

3.控制措施數量(改變名稱22項)

2022	2013	項目名稱
5.19	15.1.1	供應商關係中的資訊安全
5.20	15.1.2	供應商協議內的資訊安全要求
5.21	15.1.3	管理 ICT 供應鏈中的資訊安全
5.24	16.1.1	資訊安全事件管理規劃和準備
5.25	16.1.4	資訊安全事件的評定與決策
5.34	18.1.4	PII 的隱私和保護
6.5	07.3.1	終止或改變工作後的責任
6.7	06.2.2	遠端工作
7.1	11.1.1	實體安全邊界
7.7	11.2.9	桌面淨空與螢幕淨空
7.9	11.2.6	場外資產的安全

2022	2013	項目名稱
8.2	9.2.3	特權存取權限
8.4	9.4.5	程式源碼的存取
8.5	09.4.2	安全認證
8.7	12.2.1	防範惡意軟體
8.14	17.2.1	資訊處理設施的備援
8.20	13.1.1	網路安全
8.22	13.1.3	網路區隔
8.25	14.2.1	安全的開發生命週期
8.27	14.2.5	安全系統架構和工程原理
8.33	14.3.1	測試資訊
8.34	12.7.1	在稽核測試期間保護資訊系統

如何遵循新標準

ISO 27001:2022

如何執行轉版

1
了解
變化

2
教育
訓練

3
差異
分析

4
風險
分析

5
風險
處理

6
適用
聲明

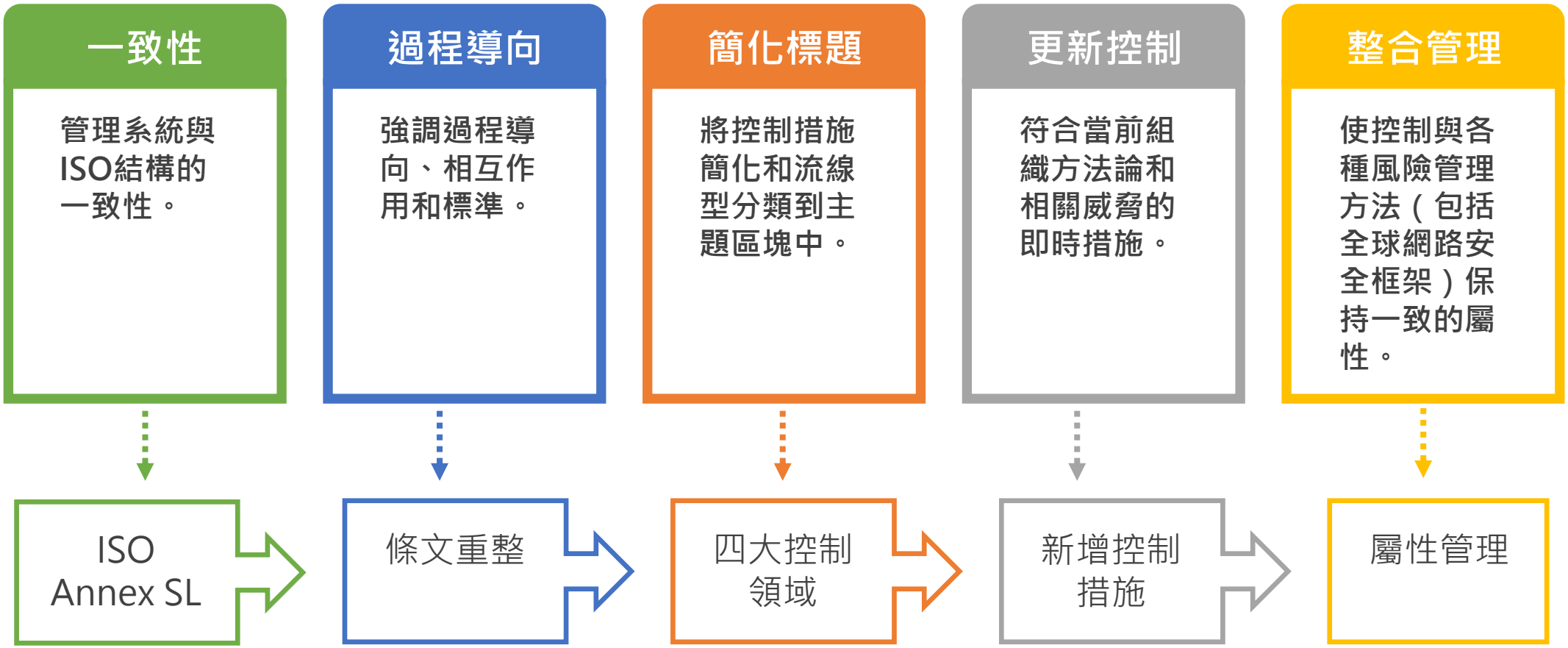
7
文件
修訂

8
執行
紀錄

9
轉版
驗證

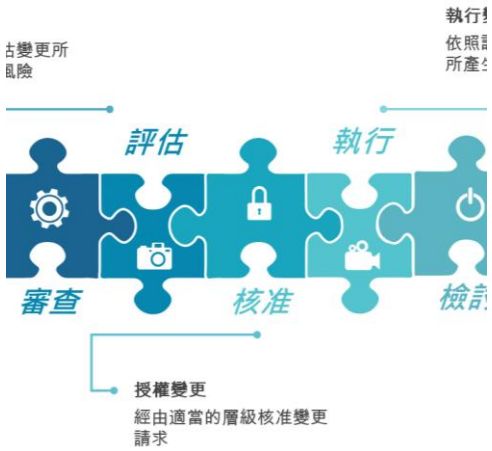
10
持續
改善

1.了解變化

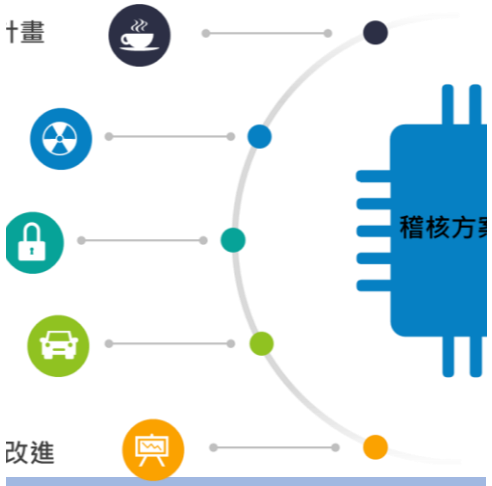

一致性
管理系統與ISO結構的一致性。
過程導向
強調過程導向、相互作用和標準。
簡化標題
將控制措施簡化和流線型分類到主題區塊中。
更新控制
符合當前組織方法論和相關威脅的即時措施。
整合管理
使控制與各種風險管理方法（包括全球網路安全框架）保持一致的屬性。
ISO Annex SL
條文重整
四大控制領域
新增控制措施
屬性管理

2.教育訓練

為您的團隊成員創建一個培訓計劃，以圍繞標準建立他們的知識，並確保他們能夠有效地實施變更。



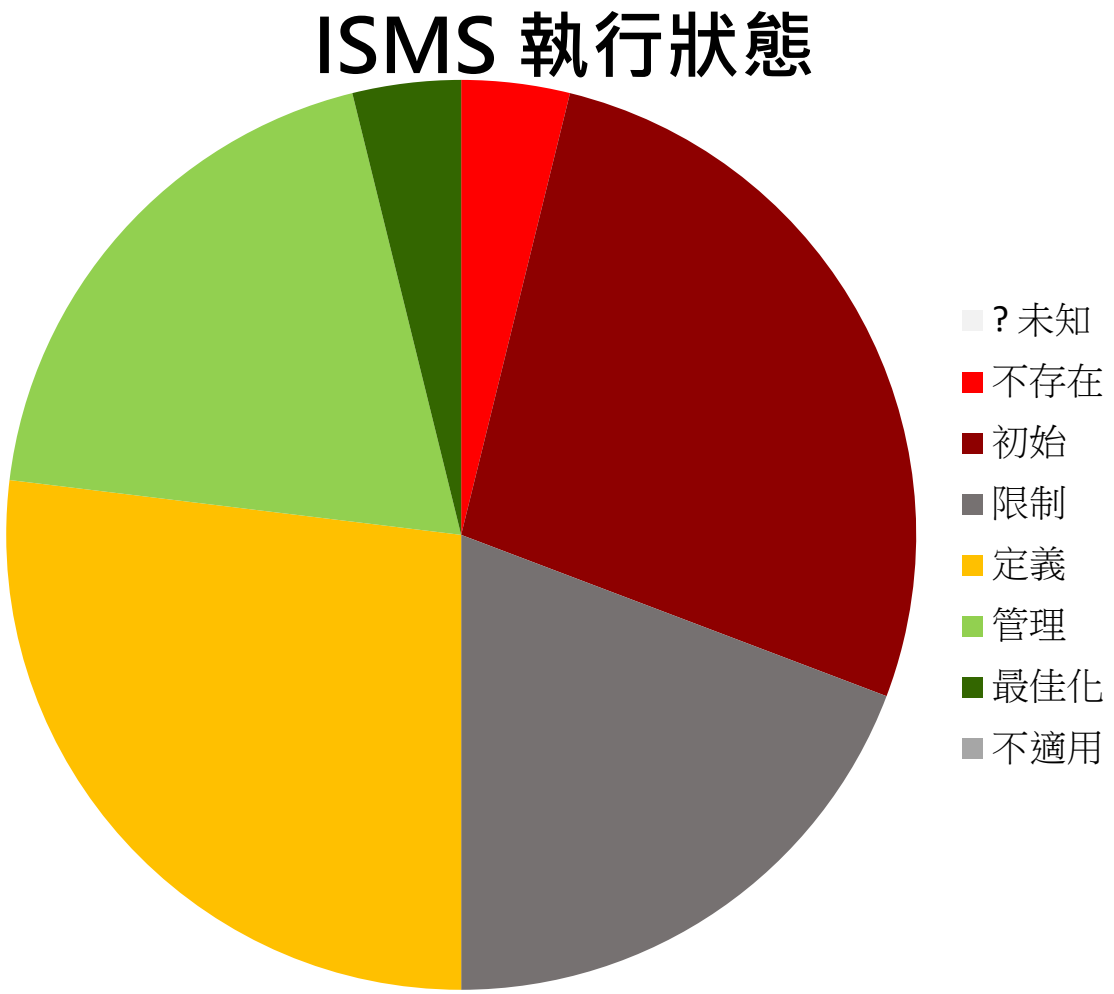
ISO 27001:2022
基礎認知
控制措施實作
變更說明

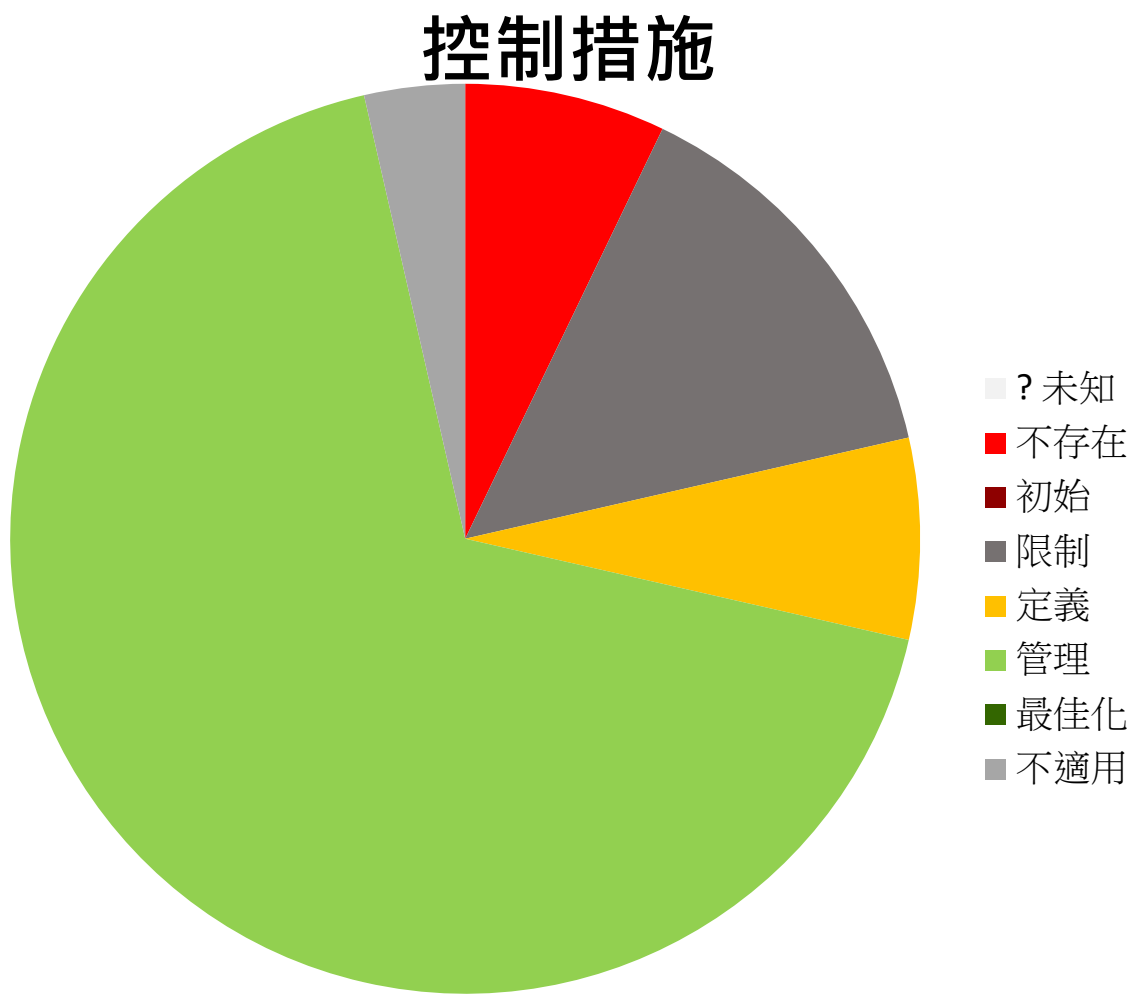


ISO 27001:2022
內部稽核

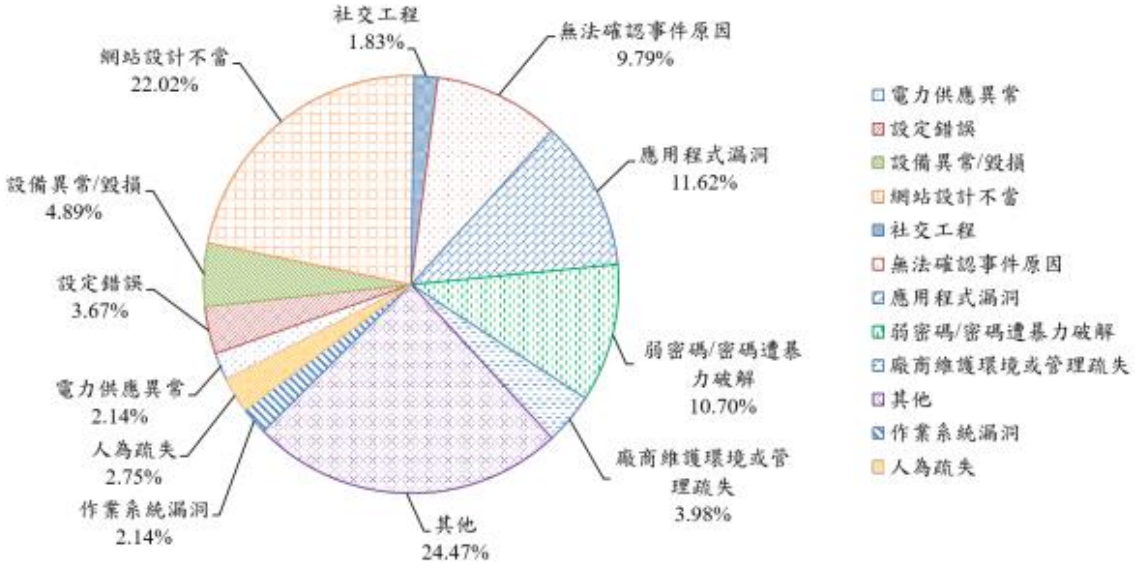
ISO 27001:2022
主導稽核員

2.差異分析


ISMS 執行狀態
? 未知
不存在
初始
限制
定義
管理
最佳化
不適用

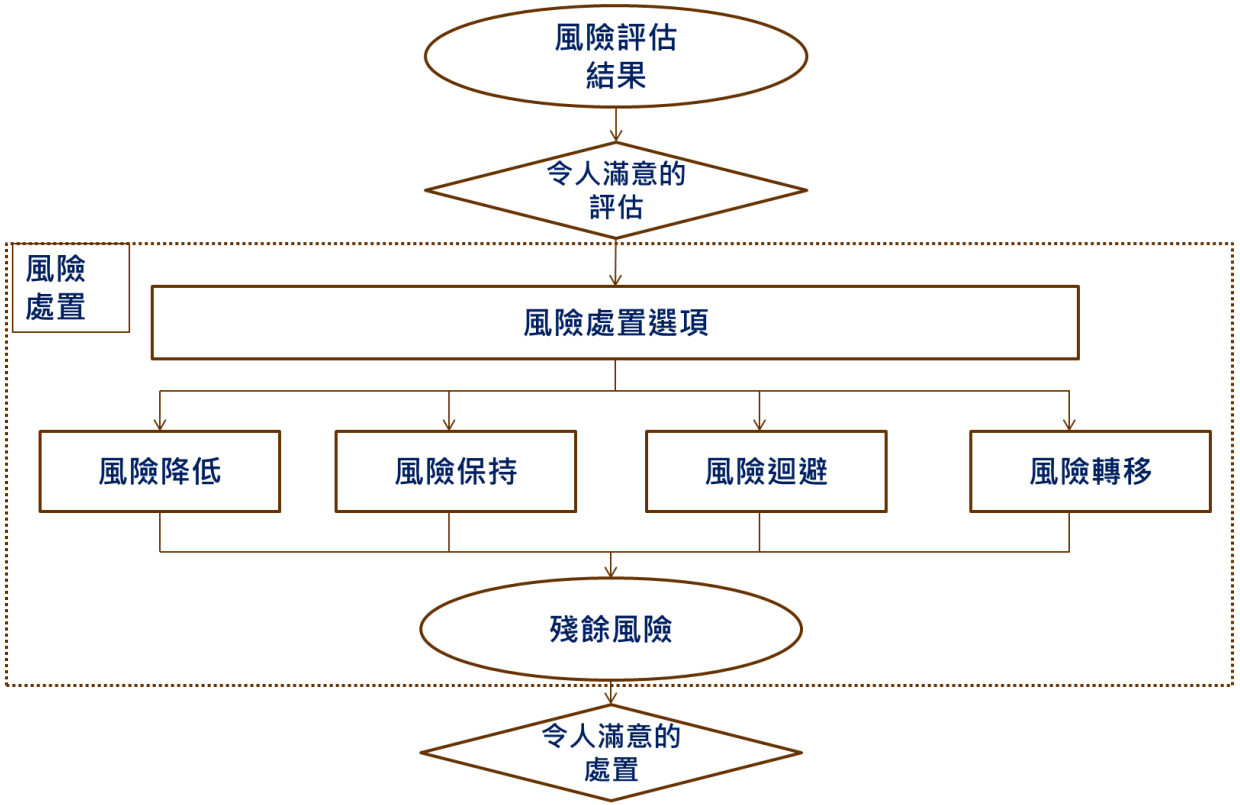

控制措施
? 未知
不存在
初始
限制
定義
管理
最佳化
不適用

4.風險分析



	威脅	低			中			高		
	弱點	低	中	高	低	中	高	低	中	高
資產價值	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	6	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

5.風險處理



Section	Information security control	Status
A5	Organizational controls	
A.5.1	資訊安全政策	限制
A.5.2	資訊安全的角色與職責	不存在
A.5.3	職務區隔	定義
A.5.4	管理階層責任	限制
A.5.5	與權責機關的聯繫	管理
A.5.6	與特殊利害關係者的聯繫	限制
A.5.7	威脅情資	限制
A.5.8	專案管理的資訊安全	限制
A.5.9	資訊和其它相關資產的盤點	限制
A.5.10	資訊和其它相關資產之可被接受的使用	初始
A.5.11	資產歸還	最佳化
A.5.12	資訊分類	管理

6.適用性聲明

		名稱	適用	參考文件	適用說明(不適用理由)
5		組織面控制措施			
5.1		資訊安全政策	適用	資訊安全政策	資訊安全政策和特定主題的政策應被定義、獲管理層核准、發布、傳達給相關人員及相關的利害關係者並取得其認可，並於計劃的時間間隔和發生重大變化時進行審查。
5.2		資訊安全的角色與職責	不適用	組織及人力管理程序	應根據組織的需要，定義和分配資訊安全角色與職責。
5.3		職務區隔	適用	組織及人力管理程序	相互衝突的職務和責任領域應被區隔。
5.4		管理階層責任	適用	組織及人力管理程序	管理階層應要求所有人員按照組織已制定的資訊安全政策、特定主題政策及程序運用資訊安全。
5.5		與權責機關的聯繫	適用	組織及人力管理程序	組織應與有關之權責機關建立並保持聯繫。
5.6		與特殊利害關係者的聯繫	適用	組織及人力管理程序	組織應與特殊利害關係者或其他專家安全論壇和專業協會建立並保持聯繫。
5.7		威脅情資	適用	資訊安全事件管理程序	應蒐集和分析與資訊安全威脅有關的資訊以產出威脅情資。
5.8		專案管理的資訊安全	適用	組織及人力管理程序	資訊安全應融入專案管理之中。
5.9		資訊和其它相關資產的盤點	適用	資產管理程序	應發展並維持資訊和其它相關資產（包括所有者）的盤點。

7.文件修訂

文件名稱	文件密等	版本	對應表單			
			表單編號	表單名稱	機密等級	版次
資訊安全政策	一般	1.0	IS-001-01	目標管控及量測表	一般	1.0
資訊安全管理程序	一般	1.0	IS-002-01	組織全景鑑別表	一般	1.0
			IS-002-02	內部稽核查檢表	一般	1.0
			IS-002-03	矯正與預防處理單	一般	1.0
			IS-002-04	管制文件一覽表	一般	1.0
			IS-002-05	外來文件一覽表	一般	1.0
			IS-002-06	文件制訂修訂及廢止申請單	一般	1.0
組織及人力管理程序	一般	1.0	IS-003-01	人員執掌及外部聯絡清單	一般	1.0
			IS-003-02	訓練規劃及紀錄表	一般	1.0
			IS-003-03	委外人員保密切結書	一般	1.0
風險評鑑管理程序	一般	1.0	IS-004-01	資產及風險評鑑表	一般	1.0
			IS-004-02	風險處理計畫	一般	1.0
資產管理程序	一般	1.0	IS-005-01	資訊資產異動申請表	一般	1.0
存取控制管理程序	一般	1.0	IS-006-01	帳號審查表	一般	1.0
			IS-006-02	資訊服務申請單	一般	1.0
實體安全管理程序	一般	1.0	IS-007-01	資訊機房進出管制表	一般	1.0
			IS-007-02	資訊機房管理紀錄表	一般	1.0
作業安全管理程序	一般	1.0	IS-008-01	備份管理作業表	一般	1.0
			IS-008-02	弱點處理作業表	一般	1.0
			IS-008-03	個人及筆記型電腦設備檢查表	一般	1.0
通訊安全管理程序	一般	1.0				
資訊系統獲取、開發及維護管理程序	一般	1.0	IS-010-01	資訊系統獲取、開發及維護管制表	一般	1.0
供應商管理程序	一般	1.0	IS-011-01	供應商評鑑表	一般	1.0
			IS-011-02	供應商保密切結書	一般	1.0
資訊安全事件管理程序	一般	1.0	IS-012-01	資訊安全事故報告單	一般	1.0
營運持續管理程序	一般	1.0	IS-013-01	業務流程營運衝擊分析表	一般	1.0
			IS-013-02	營運持續計畫演練規劃暨處理報告單	一般	1.0
遵循性管理程序	一般	1.0				
適用性聲明書	一般	1.0				

8.執行紀錄

2.1 活動和職責

此處描述管理軟體配置和職責所需的功能。

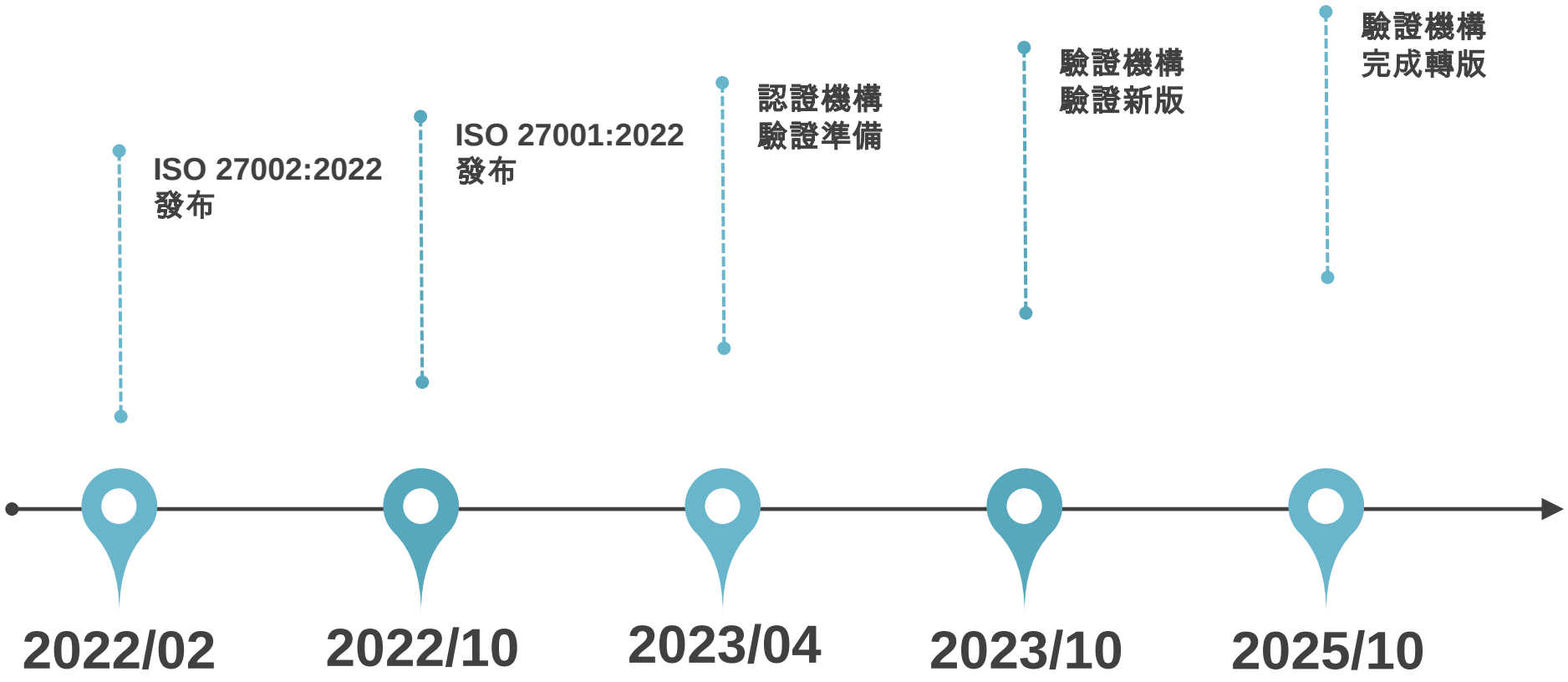
設置專案時的活動	**責任人**
標識配置項	軟體構型管理員
安裝錯誤儲存庫工具並設置資料庫	軟體構型管理員
安裝軟體配置存儲庫工具並設置資料庫	軟體構型管理員
管理和構建參考空間	軟體構型管理員
定義配置過程	軟體構型管理員

專案生命週期中的活動	**責任人**
匯出元件以進行修改、測試或交付	軟體構型管理員
在控制下設置經過驗證的元件	軟體構型管理員
創建版本，編寫版本交付文檔	軟體構型管理員
批准參考配置	專案管理人
驗證要交付的版本並授權交付	專案管理人
備份空間	軟體構型管理員
執行配置審核	品保經理
檢查配置記錄	品保經理
存檔參考版本	軟體構型管理員

威脅情資管制表

標題：	**情資來源**：
版本：	**日期**：
威脅情資說明：	
資產特徵 資產元件： 物理/地理位置： 資產使用、儲存和/或傳輸的數據類型：	

9.轉版驗證


ISO 27002:2022
發布
ISO 27001:2022
發布
認證機構
驗證準備
驗證機構
驗證新版
驗證機構
完成轉版
2022/02
2022/10
2023/04
2023/10
2025/10

新版ISO27001效益

- 保護所有形式的資訊，包括紙本、雲端和數位資訊
- 提高抵禦網路攻擊的能力
- 提供集中管理的框架，在同一架構保護所有資訊
- 確保組織範圍內的保護，包括防護基於技術的風險和其他威脅
- 應對不斷演變的安全威脅
- 減少無效防護技術的成本和支出
- 保護完整性、機密性和可用性

10.持續改善

為應對全球網路安全挑戰並提高數位信任度，發布了新的改進版本 ISO/IEC 27001。世界上最著名的資訊安全管理標準可幫助組織保護其資訊資產——在當今日益數位化的世界中至關重要。

隨著駭客開發出更先進的網路犯罪技術，網路犯罪變得越來越嚴重和復雜。世界經濟論壇的《全球網路安全展望》報告顯示，2021 年全球網路攻擊增加了 125%，有證據表明到 2022 年將持續上升。在這個瞬息萬變的環境中，領導者必須提升戰略方法應對網路風險。

當您使用 ISO/IEC 27001 時，您向利害關係者和客戶證明您致力於安全可靠地管理資訊。這是宣傳您的組織、慶祝您的成就並證明您值得信賴的好方法。

結論

ISO 27001:2022

舊版轉新版

檢視證書效期，擇定改版時機，訂定改版計畫，準備執行改版作業

將所有新版要求融入現行管理系統中，建議修訂現有程序，若有不足新增程序文件，檢討現有資源是否足夠，必要時購置新設備或軟體，以符合新版標準要求。

執行新的或變更後的管控措施，留下紀錄以證明其有效性，安排轉版驗證事宜。

選擇時機

融入新作法

確認有效

全新導入

*通過採用網路彈性的組織將迅速成為其行業的領導者並為其管理系統設定標準。**ISO/IEC 27001** 的整體方法涵蓋整個組織，人員、技術和流程都將從中受益。*

新版架構文件

以新版標準之架構建立程序文件，以全新的方式設定管理系統。

新的風險評鑑

融合場景及資產的風險評鑑（ISO 27005)，並對應新的管控措施，訂定風險處理計畫及適用性聲明書。

控制措施屬性

利用控制措施屬性，確保各項管理、法規遵循及其他要求之適用性，彈性架構各項管控措施，確認符合標準及各項要求。

THANK YOU!

Phone:
(02) 7717 9980

Email:
Edward@ingsafe.tw

Website:
https://ingsafe.tw/